REMARKS/ARGUMENTS

Claims 1-79 are pending. No claims are amended.

The Examiner has not acknowledged the IDSs that were filed **February 26, 2002, July 30, 2003, October 31, 2003, and September 23, 2004.** Applicants respectfully request acknowledgment of the above-mentioned IDSs by initialing and returning the attached copies of the same IDSs.

Claims 1-79 are rejected under 35 U.S.C.§ 103(a) as being unpatentable over **Whitehouse** (US 6,005,945) in view of White (US 6,065,117).

Claim 1 includes, among other limitations, "a scalable server system capable of communicating with the client system over a communication network comprising: a database remote from the users including information about the users; a stateless cryptographic module for authenticating the one or more users; and a plurality of security device transaction data stored in the database for ensuring authenticity of the one or more users, wherein each security device transaction data can be processed in the server system in a stateless manner."

In a **first** Office action on 3/13/03, the Examiner rejected the above claim (among other claims) under 35 U.S.C.§ 102(e) as being anticipated by **Whitehouse** alleging that Whitehouse discloses all of the above-mentioned limitations. In a first response, Applicants argued that Whitehouse does not disclose the above limitation. In a **second** Office action on 10/27/03, the Examiner rejected the above claim under 35 U.S.C.§ 103(a) as being unpatentable over **Whitehouse** in view of Lewis. In a second response, Applicants argued that Whitehouse in combination with Lewis does not disclose the above limitation.

In a **third** Office action on 6/21/04, the Examiner rejected the above claim under 35 U.S.C.§ 103(a) as being unpatentable over **Whitehouse** in view of Lewis. This Office action was designated as "non-final" on the second page of the action (PTO form 326). The applicants responded to this (non-final) action on 10/21/04 by amending some claims. In a **fourth** Office action (Advisory Action) on 11/3/4, the Examiner refused to enter the amendments because "they raise new issues that would require further consideration and/or search." The applicants responded by filing a RCE on 12/21/04.

In a **fifth** Office action on 1/7/05, the Examiner rejected the claims, including claim 1 which still had the same limitations as the above-mentioned limitations under 35 U.S.C.§ 103(a) again as being unpatentable over **Whitehouse** in view of Lewis (the same combination as the previous rejection). An interview was conducted with the Examiner on 4/19/2005. During the interview, Applicants' attorney also requested clarification as to the motivation for combining Lewis and Whitehouse. The motivation provided to combine these references in the Office Action of 1/7/2005 was that it would have been obvious to one of ordinary skill in the art to "modify the inventive concept of Whitehouse to include Lewis et al's. stateless cryptographic module for authenticating the one or more users because this would have enhance (sic) the security of the system." Applicants' attorney requested clarification as to how Lewis provided the enhanced security to Whitehouse. The Examiner indicated that he would have to further review the matter and wasn't able to provide an answer during the interview.

Subsequently, in a fifth response, Applicants summarized the interview and again argued that Whitehouse in combination with Lewis does not disclose the above limitation.

In a **sixth** Office action on 8/3/05, the Examiner rejected the above claim under 35 U.S.C.§ 103(a) as being unpatentable over **Whitehouse,** this time, in view of Devine. Consequently, Applicants filed a Notice of Appeal with a Pre-Appeal Brief Request for Review. In an Office communication dated 12/06/05, the prosecution was reopened.

Subsequently, in a **seventh** Office action dated 1/10/06 (the current Office action), the Examiner rejected the above claim under 35 U.S.C.§ 103(a) as being unpatentable over **Whitehouse,** this time, in view of **White**.

In the current Office action, similar to the Office action of 1/7/05, the examiner again states that "Whitehouse fails to teach a stateless cryptographic module for authenticating the one or more users. However, **White** teaches a system comprises a stateless cryptographic module for authenticating the one or more users (*see abstract, column 2 lines 18-54, 5 line 63-7 line 18*). Therefore, it would have been obvious to one of ordinary skill in the art the inventions was made to modify Whitehouse's system to include White's a stateless cryptographic module for authenticating the one or more users because this would have enhanced the security of the system." (Office action, page 3, first paragraph, underlining added.).

Again, the Examiner has not addressed Applicants' argument about "motivation to combine" based on enhancing the security of the Whitehouse's system. More importantly, other than citing long sections of White (e.g., abstract, column 2 lines 18-54, 5 line 63-7 line 18), the Examiner has not pointed out which specific sections of White teach each of the limitations in the rejected claims, for example, claim 1.

MPEP 707.07(d) states that "[a]n omnibus rejection of the claim 'on the references and for the reasons of record' is stereotyped and usually not informative and should therefore be avoided." However, the Examiner rejects all the pending claims over White reference in an omnibus and general manner and without mentioning any specific text, other than, a large and broad portion of White (column 5 line 63 to column 7 line 18) applied to all limitations of claim 1, as a group. See, Office action, page 3, first paragraph. In fact, most of the above cited sections describe how the server system of White handles the generation of a seed value, which has nothing to do with the rejected limitations of, for example, claim 1.

Nevertheless, Applicants respectfully submit that the combination of Whitehouse and White does not teach, nor does it suggest the claimed invention.

First, in regard to the element of "**a scalable server system capable of communicating with the client system over a communication network**," Applicants respectfully disagree with the Examiner that the system of Whitehouse includes the above limitation. Rather, Whitehouse describes a central computer 102 that includes customer database 172 and transaction database 172. There is no suggestion in Whitehouse that this central computer 102 is scalable. The Examiner points to the "one or more postal service computers 180" as the scalable server system. However, the postal service computers 180 communicate only with the central computer 102 and thus are NOT capable of communicating with the client system. Also, the postal service computers 180 do NOT include a database remote from the users including information about the users; a stateless cryptographic module for authenticating the one or more users; and a plurality of security device transaction data stored in the database, as required by claim 1.

Second, regarding the claim element of "**wherein each security device transaction data can be processed in the server system in a stateless manner**," Applicants respectfully disagree with the Examiner that the system of Whitehouse includes the above limitation.

Processing the security device transaction data in a stateless manner requires that "the application does not rely on any information about what occurred with the previous" transaction data and that each transaction data "includes all data needed to restore the PSD [transaction data] to its last known state when it is next loaded." See, for example, specification, page 8, lines 16-27. There is no mention in Whitehouse about this characteristic of the required PSD.

Firstly, Whitehouse in the cited text stresses that "Local memory 154 in the secure central computer also preferably stores: a customer database 172 of information about each of the user accounts serviced by the secure central computer 102; and a transaction database 174 for storing records concerning each postage indicium generated by the secure central computer 102." (Col. 8, lines 54-61, underlining added.). Furthermore, Whitehouse emphasizes that each central computer 102 stores data "in its customer database for each meter/user account." (Col. 10, lines 46-47, underlining added.). Therefore, it is clear that even if Whitehouse included more than one central computer, those multiple central computers would have their own customer databases 172 and transaction databases 174. Accordingly, a PSD stored and processed in a first central computer can not be processed in a second central computer, because the second central computer would not have sufficient information about that PSD and the stored PSD (in the first central computer) does not include sufficient information about what occurred with the previous transaction on that PSD, so that the second central computer would be able to process it. Consequently, that PSD is not capable of being processed in a stateless manner.

Secondly, central "computer 102 is configured to periodically replace the session key for each meter account with a new randomly generated key. The new key is sent to the end user computer in a message that is encrypted with the end user computer's public key, and is decrypted by the end user computer using the corresponding private key. . . . In yet another alternate embodiment, the new session key can be generated by requesting the end user computer to generate a public/private key pair and to send the public key to the secure central computer. The end user computer and the secure central computer can then both independently generate a new session key as a function of each computer's private key and the other computer's public key, using a well-known technique called "Diffie-Hellman" session key generation. (Col. 9, lines 40-58, underlining added.)

These central computer and user computer specific keys are stored in a database specific to that central computer. Therefore, each user computer is capable of establishing a communication link and requesting to process its PSD ONLY with a specific central computer for which the newly generated keys are stored in THAT central computer database. Therefore, the system of Whitehouse is NOT capable of processing each security device transaction data in a stateless manner.

Similarly, White, alone or in combination with Whitehouse, teach or suggest this limitation, because the system of White uses a token containing state information sent from the client to server. See, discussion about White below.

Third, regarding the element of "**a stateless cryptographic module for authenticating the one or more users**," Applicants respectfully disagree with the Examiner that White teaches the above limitation. There is no mention of a stateless cryptographic module in White. Rather, White describes a stateless server, and a method for executing stateful client requests on the stateless server using an encrypted token containing state information. This token is actually sent by the client to the server.

> Once the received token is decrypted, a determination is made if the token is valid (Block 224) by examining the state information. . . . For example, in the case where the day of the year is used to select the seed value for symmetric key generation, when the day of the year changes on the server system at midnight, any previously encrypted tokens will no longer be valid because the symmetric key generated using the new seed value will be different from the one used to encrypt it. If the state information is not valid or appears invalid because of a changed decryption key, then the requested action is not performed

> by the server and some appropriate response is provided to the client indicating the failure condition (Block 226).
>
> Col, 7, lines 1-17, underlining added.

Therefore, this invalidation of the generated token based on a new seed value teaches away from "a stateless cryptographic module for authenticating the one or more users."

Fourth, Applicants fail to see any **motivation to combine** White with Whitehouse, because each of the references are **individually complete** and functional in itself, so there would be no reason to add parts to any of them. For example, adding the stateless server of White will not enhance the security of Whitehouse system, because Whitehouse system is already using encryption to protect its data. Moreover, the references do not contain **any suggestion (express or implied) that they be combined** in the manner suggested by the Examiner. In fact, Whitehouse and White are from different fields.

In short, based on at least the above-mentioned **four arguments**, the independent claim 1 is patentable over cited references.

Independent claim 39 includes, among other limitations, "authenticating the one or more users using a scalable cryptographic module; and storing in the database a plurality of security device transaction data for ensuring authenticity of the one or more users, wherein each security device transaction data can be processed in the server system in a stateless manner." As discussed above, the combination of Whitehouse and White does not teach or suggest the above limitations. Consequently, claim 39 is also patentable over cited references.

In short, independent claims 1 and 39 are patentable in view of the cited references. Dependent claims 2-38 and 40-79 depend from claims 1 and 39, respectively and include all the limitations of their base claims and additional limitations therein. Accordingly, these claims are also allowable, as being dependent from an allowable independent claim and for the additional limitations they include therein and their allowance is requested.

In view of the foregoing remarks, it is respectfully submitted that this application is now in condition for allowance, and accordingly, reconsideration and allowance of this application are respectfully requested. If the Examiner believes that a telephone conference would be useful in moving this application forward to allowance, the Examiner is encouraged to contact the undersigned at (626) 795-9900.

Respectfully submitted,
CHRISTIE, PARKER & HALE, LLP

By
Raymond R. Tabandeh
Reg. No. 43,945
626/795-9900

RRT/clv

CLV PAS673980.1-*-04/10/06 11:39 AM